

COPY OF PAPERS  
ORIGINALLY FILED



2180  
U.S. Patent Application # 09/174,741  
Filed 12/22/00 2131

"Express Mail" mailing label number: EJ280 199 464 US

Date of Deposit: December 22, 2000

AS FILED

RECEIVED

MAY 02 2002

Technology Center 2100

PATENT  
Attorney Docket No. 7780/6  
(T00328)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
APPLICATION FOR UNITED STATES LETTERS PATENT

INVENTOR(S): THOMAS ADAMS

TITLE: METHOD AND SYSTEM FOR CALLING LINE  
AUTHENTICATION

ATTORNEYS: CARDINAL LAW GROUP  
1603 ORRINGTON AVENUE - SUITE 2000  
EVANSTON, ILLINOIS 60201  
(847) 474-8470



COPY OF PAPERS  
ORIGINALLY FILED

RECEIVED

MAY 02 2002

Technology Center 2100

~~METHOD AND SYSTEM FOR CALLING~~ LINE AUTHENTICATION

BACKGROUND OF THE INVENTION

5

1. Field Of The Invention

The present invention generally relates to computer networks, and more particularly relates to calling line authentication within an Internet environment.

10

2. Description Of The Related Art

An illustration of some basic components of an Advanced Intelligent Network (AIN) within a communication network in the form of a public switched telephone network 10 (PSTN 10) is shown in FIG. 1. Referring to FIG. 1, Service Switching Points (SSPs) 11a-11b are connected with a Signaling Transfer Point 12 and a Service Control Point (SCP) 13 by a Common Channel Signaling network 15. A subscriber line 17a connects an Internet server 20 to the SSP 11a. Subscriber lines 17b-18d connect client workstations 30a-30c to the SSP 11b. Subscriber lines 17e-17f connect client workstations 30d-30f to the SSP 11c. The SSPs 11a-11b are interconnected by trunks 16a and 16b to enable client workstations 30a-30f to establish communication links with the Internet server 20.

The Internet server 20 provides Internet services for users of client workstations 30a-30f. For access to secure services, it is sometimes necessary that the Internet server 20 have the capability to differentiate an authorized user of client workstations 30a-30f from an unauthorized user of client workstations 30a-30f.

One known authentication method involves having a user of client workstations 30a-30f input a user identification, a personal password, and an e-mail address. In response, the Internet server 20 provides an e-mail having a key for granting access to the secure services to the user. While the objective of this method is to enable the Internet server 20 to differentiate an authorized user from an unauthorized user, the Internet server 20 does not have the capability to ascertain when an unauthorized user has obtained the user identification, the personal password, and the e-mail address of an authorized user.

Preventing an unauthorized user from gaining access to the client workstations 30a-30f is more feasible and reliable than attempting to prevent an unauthorized user from obtaining the user identification, the personal password, and the e-mail address of an authorized user. Accordingly, an authentication method for an Internet server 20 predicated upon preventing an unauthorized user from gaining access to the client workstations 30a-30f is desirable.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram illustrating a prior art computer network including an Advanced Intelligent Network (AIN) system.

FIG. 2 is a diagram illustrating of an exemplary computer network system in accordance with an embodiment of the present invention.

FIG. 3 is a flow chart of a key distribution routine in accordance with another embodiment of the present invention.

## DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENT(S)

5           It is an advantage of the invention to provide method and system for restricting access to secured services provided by a dial-up server.

          Referring to FIGS. 2 and 3, SSPs 11a-11c, an SCP 44, a database 14, a firewall 40, a key server 50, and an ethernet 60 collectively comprise one embodiment of a calling line authentication system in accordance with the  
10   present invention for implementing a key distribution routine 70 in accordance with the present invention. An exemplary implementation of routine 70 involving client workstation 30a will now be described herein in conjunction with client workstations 30a-30c being authorized calling sources for a secured service of Internet server 45.

15           During a stage S72 of routine 70, SSP 11b receives a telephone number signal representative of Internet server from client workstation 30a. In one embodiment, the telephone number signal can be an 800 toll free number assigned to Internet server 45. In response, SSP 11b conventionally provides a termination attempt trigger (TAT) to SSP 11a upon receipt of the telephone  
20   number signal during a stage S74 of routine 70. The TAT identifies a directory number representative of client workstation 30a, and is therefore an indication to SSP 11a that client workstation 30a wishes to establish a communication link with Internet server 45. In response to the TAT, SSP 11a provides a query to SCP 44 that includes an authorization for establishing the  
25   communication link between client workstation 30a and Internet server 45.

          Database 14 of the telephone network 42 stores a list of directory numbers having authorization to access the secured service on Internet server 45, and a corresponding plurality of authentication keys for granting access to the secured service on Internet server 45. In response to the query,  
30   SCP 44 searches the list of authorized directory numbers in database 14 for

the directory number of client workstation 30a during a stage S76 of routine 70. Upon detection of the directory number, SCP 44 retrieves one of the authentication keys from database 14.

5           During a stage S78 of routine 70, SCP 44 conventionally directs SSP 11a and SSP 11b to establish the communication link between client workstation 30a and Internet server 45.

          During a stage S80 of routine 70, SCP 44 provides the retrieved authentication key to key server 50 via firewall 40 and ethernet 60. Key  
10   server 50 in turn provides the retrieved authentication key to Internet server 45. In one embodiment, Internet server 45 queries key server 50 for the authentication key upon an establishment of the communication link between client workstation 30a and Internet server 45. In another embodiment, key  
15   server 50 provides the authentication key to Internet server 45 upon a detection of the establishment of the communication link between client workstation 30a and Internet server 45. During a stage S82 of routine 70, key  
SCP 44 removes the retrieved authentication key from key server 50.

          An exemplary implementation of routine 70 involving client workstation 30d will now be described herein in conjunction with client  
20   workstations 30a-30c being unauthorized calling sources for secured services of Internet server 45, and client workstations 30d-30f being unauthorized calling sources for secured services of Internet server 45.

          During stage S72 of routine 70, SSP 11c receives a telephone number signal representative of Internet server 45 from client workstation 30d. In  
25   response, SSP 11c conventionally provides a termination attempt trigger (TAT) to SSP 11a upon receipt of the telephone number signal during stage S74 of routine 70. The TAT identifies a directory number representative of client workstation 30d, and is therefore an indication to SSP 11a that client workstation 30d wishes to establish a communication link with Internet server

45. In response to the TAT, SSP 11a provides a query to SCP 44 that includes an authorization for establishing the communication link between client workstation 30d and Internet server 45.

5 Database 14 stores a list of directory numbers having authorization to access the secured service on Internet server 45, and a corresponding plurality of authentication keys for granting access to the secured service on Internet server 45. In response to the query, SCP 44 searches the list of authorized directory numbers in database 14 for the directory number of client  
10 workstation 30d during stage S76 of routine 70. Routine 70 is terminated upon a failure to detect the directory number of client workstation 30d within database 14, and the client workstation 30d is denied access to the Internet server 45.

From the preceding two exemplary illustrations of routine 70, one  
15 advantage of the present invention is the distribution of authentication keys to only authorized client workstations 30a-30c as identified in database 14. Another advantage of the present invention is the prevention of granting access of secured services of Internet server 45 to a user, authorized or unauthorized, of client workstations 30d-30f despite the user having the  
20 correct telephone number for Internet server 45.

While the embodiments of the present invention disclosed herein are presently considered to be preferred, various changes and modifications can be made without departing from the spirit and scope of the invention. The scope of the invention is indicated in the appended claims, and all changes  
25 that come within the meaning and range of equivalents are intended to be embraced therein. For example, the present invention can be implemented with a different type of intelligent network other than an AIN, or with different or additional components of an AIN. Also, other calling sources can be

incorporated into the present invention including, but not limited to, cellular telephones, wireless units, or the like, and other calling destinations other than an Internet server can be incorporated into the present invention.